



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/875,723	06/06/2001	Isabelle Jussy	560043670106	7175

7590

11/02/2004

F. Drexel Feeling  
Jones, Day, Reavis & Pogue  
North Point  
901 Lakeside Avenue  
Cleveland, OH 44114

EXAMINER

BAUM, RONALD

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 11/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

88

124

## Office Action Summary

Application No.

09/875,723

Applicant(s)

JUSSY ET AL.

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) \*
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 10142004.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_.

**DETAILED ACTION**

1. Claims 1-36 are pending for examination.
2. Claims 1-36 are rejected.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 1-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1,5 (and respectively 2-4,6-21 by dependency), recite a “network element” comprising a “an algorithm ...”. This appears to be software method claim language that is non-statutory per se. Also, the claim language does not explicitly specify a software (i.e., the software embodiment of a function, method, etc.,) or hardware system. The examiner assumes for the sake of applying art that the claim refers to embodied software method. Correction is required.

4. Claims 21,22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 21,22 recite a “network element” comprising a “... software program ...”. This appears to be software method claim language that is non-statutory per se. The examiner assumes for the sake of applying art that the claim refers to embodied software method. Correction is required.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-7,16-18,21-26,34 are rejected under 35 U.S.C. 102(e) as being anticipated by Cromer et al, U.S. Patent 6,609,207 B1.

6. As per claim 1; "A network element having a plurality of features wherein at least one of the features may be optionally enabled or disabled, the network element comprising: a service module that provides a first network feature that may be optionally enabled or disabled [i.e., col. 1,lines 55-col. 5,line 35]; a system processor that is operable to receive a softkey value inputted from outside of the network element [i.e., col. 1,lines 55-col. 5,line 35]; and a softkey validation system that is operable to enable the use of the first network feature when the received softkey value is the same as a first valid softkey value, the softkey validation system also being operable to enable the use of the first network feature a second time, after the first network feature has been deactivated, when the received softkey value is the same as a second valid softkey value, wherein the first valid softkey value is not the same as the second valid softkey value, the softkey validation system comprising: memory for storing information related to the service module [i.e., col. 1,lines 55-col. 5,line 35]; and an algorithm for use in confirming whether the received

Art Unit: 2136

softkey value is a valid softkey value; and wherein upon confirmation that the received softkey value is valid the softkey validation system enables the use of the network feature [col. 1, lines 55-col. 7, line 31, whereas the use of separate connection and disconnect passwords are broadly interpreted by the examiner to correspond to the applicants 2 (different) softkeys used in the 'softkey validation system' elements, and further, the laptop docked to the docking station which itself is interfaced to a network (i.e., Ethernet interfacing) is broadly interpreted by the examiner to correspond to the applicants 'network element having a plurality of features ... enabled or disabled, ... a service module that provides a first network feature ...', 'memory for storing information related to the service module', 'an algorithm (assumed embodied software, etc.) ... confirming ... a valid softkey value; and ... upon confirmation ... system enables the use of the network feature', and '... system processor ... to receive a softkey value inputted from outside of the network element'.].”;

Further, as per claim 5; “A node element in a communication network, comprising: a service module that provides a first network feature that may be optionally enabled or disabled [i.e., col. 1, lines 55-col. 5, line 35]; a system processor that is operable to receive a softkey value inputted from outside of the network element [i.e., col. 1, lines 55-col. 5, line 35]; and a softkey validation system that is operable to enable the use of the first network feature when the received softkey value is the same as a first valid softkey value, the softkey validation system also being operable to enable the use of the first network feature a second time, after the first network feature has been deactivated, when the received softkey value is the same as a second valid softkey value, wherein the first valid softkey value is not the same as the second valid softkey value, the softkey validation system comprising: memory for storing information related to the

Art Unit: 2136

service module [i.e., col. 1, lines 55-col. 5, line 35]; and an algorithm for use in confirming whether the received softkey value is a valid softkey value [i.e., col. 1, lines 55-col. 5, line 35]; and wherein upon confirmation that the received softkey value is valid the softkey system enables the use of the network feature [This claim is claim 1 from the point of view of the 'node element in a communication network' type of network per se, and the docking station / laptop / security processor of Cromer et al clearly encompasses a communications network configuration, and is rejected for the same reasons provided for the claim 1 rejection].”;

Further, as per claim 23; “A system for enabling the use of network features in a network element, comprising a softkey assignment system that is operable to perform operations with respect to at least one softkey, the softkey assignment system being operable to assign a softkey value to the softkey and to update the softkey status to an assigned state upon the assignment of a softkey value to the softkey, the softkey assignment system also being operable to update the softkey status to an unassigned state upon the receipt of a deactivate softkey value for the softkey [i.e., col. 1, lines 55-col. 5, line 35]; and a network element, the network element comprising: a service module that provides a. first network feature that may be optionally enabled or disabled [i.e., col. 1, lines 55-col. 5, line 35]; and a softkey validation system that is operable to enable the use of the first network feature when a received softkey value is the same as a first valid softkey value [This claim is claim 1 from the point of view of the setup / configuration of the softkeys, and the docking station / laptop / security processor of Cromer et al clearly encompasses the setup of the passwords for connect / disconnect / relocation, and is rejected for the same reasons provided for the claim 1 rejection].”;

Further, as per claim 34; “A method for authorizing the use of a network feature in a network, the network comprising a softkey assignment system, and a network element comprising a service module that provides a first network feature that may be optionally authorized, the method comprising the steps of: allowing a customer to use the first network feature [i.e., col. 1, lines 55-col. 5, line 35]; generating an alarm condition when the customer uses the first network feature without supplying a softkey value [i.e., col. 1, lines 55-col. 5, line 35]; providing a customer with a softkey upon request by the customer [i.e., col. 1, lines 55-col. 5, line 35]; generating the softkey value for the softkey [i.e., col. 1, lines 55-col. 5, line 35]; providing the softkey value to the customer upon request by the customer; and canceling the alarm condition in response to the customer supplying the softkey value to the network element [This claim is the method claim for the system claim 23 from the point of view of the setup / configuration of the softkeys, and for ‘the generating an alarm condition’ and the responses to such alarm conditions, such that the docking station / laptop / security processor of Cromer et al clearly encompasses the responses (i.e., the disable / enabling states of the laptop and docking station) upon correct / incorrect password entry at pre / post docking scenarios, and is rejected for the same reasons provided for the claim 1, 23 rejections].”.

7. Claim 2 *additionally recites* the limitation that; “The network element according to claim 1 wherein enabling the use of the network feature comprises enabling the use of the network feature without the generation of alarms.”. The teachings of Cromer et al suggest such limitations (col. 1, lines 55-col. 7, line 31, whereas the laptop docked to the docking station successfully (post correct password entry, thereby enabling appropriate laptop / docking station interfacing

Art Unit: 2136

functionality) is interfaced to a network (i.e., Ethernet interfacing) is broadly interpreted by the examiner to correspond to the applicants 'enabling the use of the network feature without the generation of alarms' element.).

8. Claim 3 *additionally recites* the limitation that; "The network element according to claim 1 wherein enabling the use of the network feature comprises enabling the use of the network feature when the network feature could not be used, even in an alarm state, without being enabled through the softkey system.". The teachings of Cromer et al suggest such limitations (col. 1, lines 55-col. 7, line 31, whereas the laptop docked to the docking station successfully (post correct password entry, thereby enabling appropriate laptop / docking station interfacing functionality) is interfaced to a network (i.e., Ethernet interfacing) is broadly interpreted by the examiner to correspond to the applicants 'enabling the use of the network feature when the network feature could not be used, even in an alarm state, without being enabled through the softkey system' element, in that the connect or relocation passwords allow restoration of proper functionality given correct password entry.).

9. Claim 4 *additionally recites* the limitation that; "The network element according to claim 1 wherein the algorithm is operable for generating a deactivated softkey value when the first network feature has been deactivated.". The teachings of Cromer et al suggest such limitations (col. 1, lines 55-col. 7, line 31, whereas the scenario involving the relocation password causing the docking station loss of power insofar as docking station functions, inclusive of powering up memory that would contain the password information (thereby rendering the password



effectively 'erased'), is broadly interpreted by the examiner to correspond to the applicants 'the algorithm is operable for generating a deactivated softkey value when the first network feature has been deactivated' element, in that the connect or relocation passwords *would* allow restoration of proper functionality given correct password entry.).

10. Claim 6 ***additionally recites*** the limitation that; "The node element according to claim 5 wherein the service module is a communication module.". The teachings of Cromer et al suggest such limitations (col. 1, lines 55-col. 7, line 31, whereas the use of a 'service module is a communication module' type of configuration per se, is such that the docking station / laptop / security processor of Cromer et al clearly encompasses communication modules in that the laptop has a communications channel to the docking station that has an external network connection.).

11. Claim 7 ***additionally recites*** the limitation that; "The node element according to claim 6 wherein the first network feature is a communication port.". The teachings of Cromer et al suggest such limitations (col. 1, lines 55-col. 7, line 31, whereas the use of a 'first network feature is a communication port' type of configuration per se, is such that the docking station / laptop / security processor of Cromer et al clearly encompassing communication modules inherently using communication ports, in that the laptop has a communications channel to the docking station that has an external network connection, all of which is via the said associated communication ports. Further, said communications via the port(s) is such that if the laptop /

docking station is not enabled via appropriate password invocation, clearly the communications (via a communications port) as a 'first network feature' will not likewise be enabled.).

12. Claim 16 ***additionally recites*** the limitation that; "The node element according to claim 7 wherein the first network feature is an Ethernet port.". The teachings of Cromer et al suggest such limitations (i.e., col. 3, lines 55-col. 4, line 4).

13. Claim 17 ***additionally recites*** the limitation that; "The node element according to claim 7 wherein the first network feature is a Fast Ethernet port.". The teachings of Cromer et al suggest such limitations (i.e., col. 3, lines 55-col. 4, line 4).

14. Claim 18 ***additionally recites*** the limitation that; "The node element according to claim 7 wherein the first network feature is a Gigabit Ethernet port.". The teachings of Cromer et al suggest such limitations (i.e., col. 3, lines 55-col. 4, line 4).

15. Claim 21 ***additionally recites*** the limitation that; "The node element according to claim 5 wherein the service module is a software program.". The teachings of Cromer et al suggest such limitations (col. 1, lines 55-col. 7, line 31, whereas the use of a 'service module is a software program' type of configuration per se, is such that the docking station / laptop / security processor of Cromer et al clearly encompasses software modules in that the laptop is operable by software / firmware and communicates / verifies passwords related to the docking station that

Art Unit: 2136

likewise is operable by software / firmware and communicates / verifies passwords as part of functionality that is itself a network function enabled /disabled appropriately.).

16. Claim 22 ***additionally recites*** the limitation that; “The node element according to claim 21 wherein the first network feature is an output from the software program. ”. The teachings of Cromer et al suggest such limitations (col. 1,lines 55-col. 7,line 31, whereas the use of a ‘first network feature is an output from the software program’ type of configuration per se, is such that the docking station / laptop / security processor of Cromer et al clearly encompasses software modules in that the laptop is operable by software / firmware and communicates / verifies passwords related to the docking station that likewise is operable by software / firmware and communicates / verifies passwords as part of functionality that is itself a network feature (function enabled /disabled appropriately).).

17. Claim 24 ***additionally recites*** the limitation that; “The system according to claim 23 wherein the service module includes the softkey validation system.”. The teachings of Cromer et al suggest such limitations (col. 1,lines 55-col. 7,line 31, whereas the use of separate connection and disconnect passwords are broadly interpreted by the examiner to correspond to the applicants 2 (different) softkeys used in the ‘service module includes the softkey validation system’ elements.).

18. Claim 25 ***additionally recites*** the limitation that; “The system according to claim 23 wherein the network element further comprises a shelf processor and wherein the shelf processor

Art Unit: 2136

includes the softkey validation system.”. The teachings of Cromer et al suggest such limitations (col. 1, lines 55-col. 7, line 31, whereas the use of a laptop that is inserted into a docking station is broadly interpreted by the examiner to correspond to the applicants ‘a shelf processor and wherein the shelf processor includes the softkey validation system’ elements.).

19. Claim 26 *additionally recites* the limitation that; “The system according to claim 23 wherein the service module comprises an internal counter and wherein the internal counter stores a value that is used by the softkey validation system in determining whether the received softkey value is valid.”. The teachings of Cromer et al suggest such limitations (col. 1, lines 55-col. 7, line 31, whereas the use of memory (or a latch, in the case of the relocation scenario) to effect storage of the state of the password entry process, is broadly interpreted by the examiner to correspond to the applicants ‘internal counter ... counter stores a value that is used by the softkey validation system ... softkey value is valid’ elements, in that although a latch / memory may retain the persistent state of a single process, the count of the persistent state, although only 2 states, is a count none the less.).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2136

20. Claims 8-15,19,20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al, U.S. Patent 6,609,207 B1 as applied to claim 5 above, and further in view of below.

Claim 8 ***additionally recites*** the limitation that; “The node element according to claim 7 wherein the first network feature is a OC-3 port.”;

Claim 9 ***additionally recites*** the limitation that; “The node element according to claim 7 wherein the first network feature is a OC-12 port.”;

Claim 10 ***additionally recites*** the limitation that; “The node element according to claim 7 wherein the first network feature is a OC-48 port.”;

Claim 11 ***additionally recites*** the limitation that; “The node element according to claim 7 wherein the first network feature is a OC-192 port.”;

Claim 12 ***additionally recites*** the limitation that; “The node element according to claim 7 wherein the first network feature is a EC-1 port.”;

Claim 13 ***additionally recites*** the limitation that; “The node element according to claim 7 wherein the first network feature is a DS3 port.”;

Claim 14 ***additionally recites*** the limitation that; “The node element according to claim 7 wherein the first network feature is a DS1 port.”;

Claim 15 ***additionally recites*** the limitation that; “The node element according to claim 7 wherein the first network feature is a E1 port.”;

Claim 19 ***additionally recites*** the limitation that; “The node element according to claim 5 wherein the service module is an optical mapper.”;

Claim 20 *additionally recites* the limitation that; “The node element according to claim 19 wherein the first network feature is an optical network port.”.

The teachings of Cromer et al suggest the base claim (“A node element in a communication network, comprising: a service module that provides a first network feature that ... enabled or disabled; a system processor ... to receive a softkey ... a softkey validation system ... to enable the use of the first network feature ..., the softkey validation system comprising: memory ... an algorithm for use ... valid softkey value... confirmation ...”) limitations (col. 1, lines 55-col. 7, line 31) *without explicitly teaching* of the use of the various specific communications interfaces.

The limitations concerning the use of the various communications interfaces are broadly interpreted by the examiner to correspond to design choices by the applicant insofar as the communications applications / networks are driven by the general nature of the network protocol (i.e., logical and electrical).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Cromer et al ‘... node element in a communication network ...’, with the various interfaces.

Such motivation to combine would clearly encompass the need to allow for compatibility with whatever generally specified network interface is being considered (i.e., Cromer et al, col. 3, line 64-col. 4, line 13).

21. Claims 27-33, 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al, U.S. Patent 6,609,207 B1, and further in view of Mufic, U.S. Patent 5,943,423.

As per claim 27; “A method for enabling the use of network features in a network element within a network, the network element comprising a service module that provides a first network feature that may be optionally enabled, the method comprising the steps of: receiving an encrypted softkey value from outside of the network element; decrypting the encrypted softkey value; determining whether the received softkey value is equal to a first valid softkey value; enabling the first network feature if the received softkey value is equal to the first valid softkey value; and providing a mechanism for deriving a second valid softkey value wherein the second valid softkey value is not equal to the first valid softkey value, wherein the second valid softkey value is operative to allow the first network feature to be activated if the first network feature is deactivated after it has been activated using the first valid softkey value, and wherein the first valid softkey value is not operative to allow the first network feature to be activated again if the first network feature is deactivated after it has been activated using the first valid softkey value.”;

The teachings of Cromer et al suggest the base claim (“A method for enabling the use of network features in a network element ... comprising a service module ... comprising the steps of: receiving an encrypted softkey; ... decrypting ... softkey value; determining ... equal to a ... value; enabling the first network feature ...”) limitations (col. 1, lines 55-col. 7, line 31) *without explicitly teaching* of the use of the various encryption / decryption functions involved with the softkey.

Mufic teaches of using encrypted parameters to access a client network node (i.e., element of the network) utilizing smartcard or such token credentials, inclusive of sending the client an encrypted password that is decrypted by the client network node (col. 5, line 23-col. 6, line 20, col. 7, line 60-col. 11, line 13).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Cromer et al 'A method for enabling the use of network features in a network element ...', with the various encryption / decryption functions involved with the softkey.

Such motivation to combine would clearly encompass the need to allow secure transfer of the password (softkey) from an external source to the network element insofar as the whole point of having the passwords is to assure the confidentiality of the passwords so that they can be used for the specified security servicing related to the invention (i.e., Cromer et al, col. 3, lines 1-12).

22. As per claim 28; "A method for enabling the use of network features in a network, the network comprising a softkey assignment system, and a network element comprising a service module that provides a first network features that may be optionally enabled, the method comprising the steps of: providing a customer with a reusable softkey; generating with the softkey assignment system a softkey value for the softkey; encrypting the softkey value; assigning the encrypted softkey value to the softkey; providing the encrypted softkey value to the customer upon the customer's request to use the softkey; updating the state of the softkey to an assigned state upon assigning the encrypted softkey value to the softkey; providing within the network element a validation system that is operable to: (a) receive an encrypted softkey value from outside of the network element, (b) decrypt the encrypted softkey value, (c) determine whether the received softkey value is equal to a first valid softkey value, and (d) enable the first network feature if the received softkey value is equal to the first valid softkey value; providing with the service module a system for deriving a second valid softkey value wherein the second



valid softkey value is not equal to the first valid softkey value, wherein the second valid softkey value is operative to allow the first network feature to be activated if the first network feature is deactivated after it has been activated using the first valid softkey value, and wherein the first valid softkey value is not operative to allow the first network feature to be activated again if the first network feature is deactivated after it has been activated using the first valid softkey value; providing a method for allowing the customer to return the softkey to an unassigned state; and allowing the customer to re-use the softkey for activating a second network feature by allowing the softkey assignment system to provide the customer with a second softkey value upon request if the softkey is in an unassigned state at the time of the request [This claim is the method claim for the system claim 23 from the point of view of the use of the various encryption / decryption functions involved with the softkey as rejected above in the claim 27 rejection, and is rejected for the same reasons provided for the claim 1, 23, and 27 rejections].”.

23. Claim 29 *additionally recites* the limitation that; “The method of claim 28 wherein the providing a method for allowing the customer to return the softkey step comprises the steps of: providing within the network element a system for deactivating the feature associated with the installed softkey and for returning to the customer a deactivation key value upon deactivation of the feature; accepting the deactivation key value from the customer; and updating the state of the softkey to reflect that it is in an unassigned state [This claim is the method claim for the system claim 4 from the point of view of the use of the various encryption / decryption functions involved with the softkey as rejected above in the claim 28 rejection, and is rejected for the same reasons provided for the claim 4,28 rejections].”.

24. Claim 30 ***additionally recites*** the limitation that; “The method of claim 28 wherein the system for deriving a second valid softkey value comprises a counter within the service module that keeps track of the number of times that the service module feature has been deactivated [This claim is the method claim for the system claim 26 from the point of view of the use of the various encryption / decryption functions involved with the softkey as rejected above in the claim 28 rejection, and is rejected for the same reasons provided for the claim 26,28 rejections].”.

25. Claim 31 ***additionally recites*** the limitation that; “The method of claim 28 wherein the system for deriving a second valid softkey value comprises a counter within the service module that keeps track of the number of times that the service module feature has been activated [This claim is the method claim for the system claim 26 from the point of view of the use of the various encryption / decryption functions involved with the softkey as rejected above in the claim 28 rejection, and is rejected for the same reasons provided for the claim 26,28 rejections].”.

26. Claim 32 ***additionally recites*** the limitation that; “The method of claim 28 wherein the service module comprises a key holding location and wherein the first network feature is enabled by loading at least a portion of the valid key value into the key holding location [This claim is the method claim for the system claim 26 from the point of view of the use of the various encryption / decryption functions involved with the softkey, and further, in that since the

Art Unit: 2136

processing elements involved all clearly have memory associated with said processing elements, the 'key holding location' correspond to these memory elements, and as such, is rejected for the same reasons provided for the claim 26,28 rejections].”.

27. Claim 33 *additionally recites* the limitation that; “The method of claim 28 wherein the service module comprises a key holding location and wherein the first network feature is enabled by loading data derived from at least a portion of the valid key value into the key holding location [This claim is the method claim for the system claim 26 from the point of view of the use of the various encryption / decryption functions involved with the softkey, and further, in that since the processing elements involved all clearly have memory associated with said processing elements, the 'key holding location' correspond to these memory elements, and as such, is rejected for the same reasons provided for the claim 26,28 rejections].”.

29. Claim 35 *additionally recites* the limitation that; “The method of claim 34 wherein the softkey value is encrypted and wherein the network element comprises a validation system that is operable to: (a) receive the encrypted softkey value from outside of the network element, (b) decrypt the encrypted softkey value, (c) determine whether the received softkey value is equal to a first valid softkey value, and (d) authorize the use of the first network feature if the received softkey value is equal to the first valid softkey value [This claim is the method claim for the system claim 23 from the point of view of the use of the various encryption / decryption functions involved with the softkey as rejected above in the claim 27 rejection, and is rejected for the same reasons provided for the claim 1, 23, and 34 rejections].”.

29. Claim 36 *additionally recites* the limitation that; “The method of claim 35 wherein the service module comprises a system for deriving a second valid softkey value wherein the second valid softkey value is not equal to the first valid softkey value, wherein the second valid softkey value is operative to allow the first network feature to be authorized if the first network feature is de-authorized after it has been authorized using the first valid softkey value, and wherein the first valid softkey value is not operative to allow the first network feature to be authorized again if the first network feature is de-authorized after it has been authorized using the first valid softkey value [This claim is the method claim for the system claim 23 from the point of view of the use of the various encryption / decryption functions involved with the softkey as rejected above in the claim 27 rejection, and is rejected for the same reasons provided for the claim 1, 23, and 35 rejections].”.

### ***Conclusion***

30. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.


Ronald Baum

Application/Control Number: 09/875,723

Page 20

Art Unit: 2136

Patent Examiner

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100